King County
Elections

Security Plan
January 21, 2009

Table of Contents

Introduction

Security of the voting process is paramount to ensuring the public's confidence in elections. The King County Elections Security Plan is intended to provide a general overview of tasks as well as roles and responsibilities of selected offices and agencies in maintaining the security of the voting process.

In general, elections systems are almost universally composed of two (2) major independent systems that provide functionality for Election Management / Voter Registration and Vote Tabulation. King County Elections employs two such systems. The system used for election management / voter registration is the Data Information Management System (DIMS). The system used to conduct ballot tabulation is the Global Election Management System (GEMS). Recently King County Elections added a third (3) component, a returned mail ballot packet sorting and data capture system. The system used in King County for this function in the Relia-Vote system from Pitney Bowes.

The Elections Director has the authority and responsibility to ensure that all employees working in elections are working in a safe environment. In addition, it is crucial that every vote be counted and that the voting process is secure. The Superintendent of Elections or his or her designee is responsible for overall coordination of security concerns during elections. That position will be clearly identified to all employees as the primary point of coordination of security issues.

Effective security does not rely on a single process, feature, or policy. Effective security requires a number of interrelated processes, systems, and policies that complement and build on each other. The systems, process and policies that comprise layers of security for King County Elections are represented in figure 1 on page 3.

These multiple layers of security systems, processes and/or procedures ensure that elections are not inappropriately influenced. External stakeholders such as the media, party observers, Elections oversight groups, the Office of the Secretary of State and the public provide transparency and are integral to the detection of problems with the elections process. The physical and personnel security measures which have been implemented ensure that only authorized individuals are allowed access to critical election spaces, materials, technical systems and ballots. Elections staff and volunteers are trained in elections processes and procedures designed to ensure the security and integrity of the election process. These elections processes are audited and reviewed throughout with many checkpoints for accuracy. This layered approach ensures that if one or even two layers are compromised, bypassed or proven ineffective the security and integrity of the election process is still preserved.

The contents of this plan are structured to parallel the layers of security shown in figure 1: open and transparent elections environment, physical and personnel security, legal and procedural security, and technical and systems security.

This plan's focus is on the policies and higher-level processes and procedures that are needed to ensure a secure election environment. Detailed processes and procedures that implement these policies will be the subject of specific guidance documents contained in the Election Section's Procedure Document Control Tree (available upon request through the office of the Superintendent of Elections or the Elections Director's Office).

The security plan is a dynamic, living document that will be reviewed biennially and updated as significant security issues arise or situations change. After every election, King County Elections staff review the lessons learned from that election and make adjustments to processes, procedures, and systems to improve the effectiveness of operations and security. The King County Elections staff also monitors the experiences of other jurisdictions and scrutinizes studies and reviews by third parties. They then adjust policies and procedures in order to avoid weaknesses experienced or identified by others.

All employees who work in elections or who have a role in elections security share responsibility to ensure that our elections remain secure and that they are conducted with the utmost integrity. To this end, all new employees are required to read and become familiar with this Security Plan as well as any implementation procedures that are relevant to their work areas. All employees will be briefed periodically with the key aspects of this plan. All employees, not just managers, are encouraged to suggest ways to improve the security of the election process. King County Elections also welcomes suggestions from oversight committees and other observers on ways to enhance system security.

Layers of Election Security

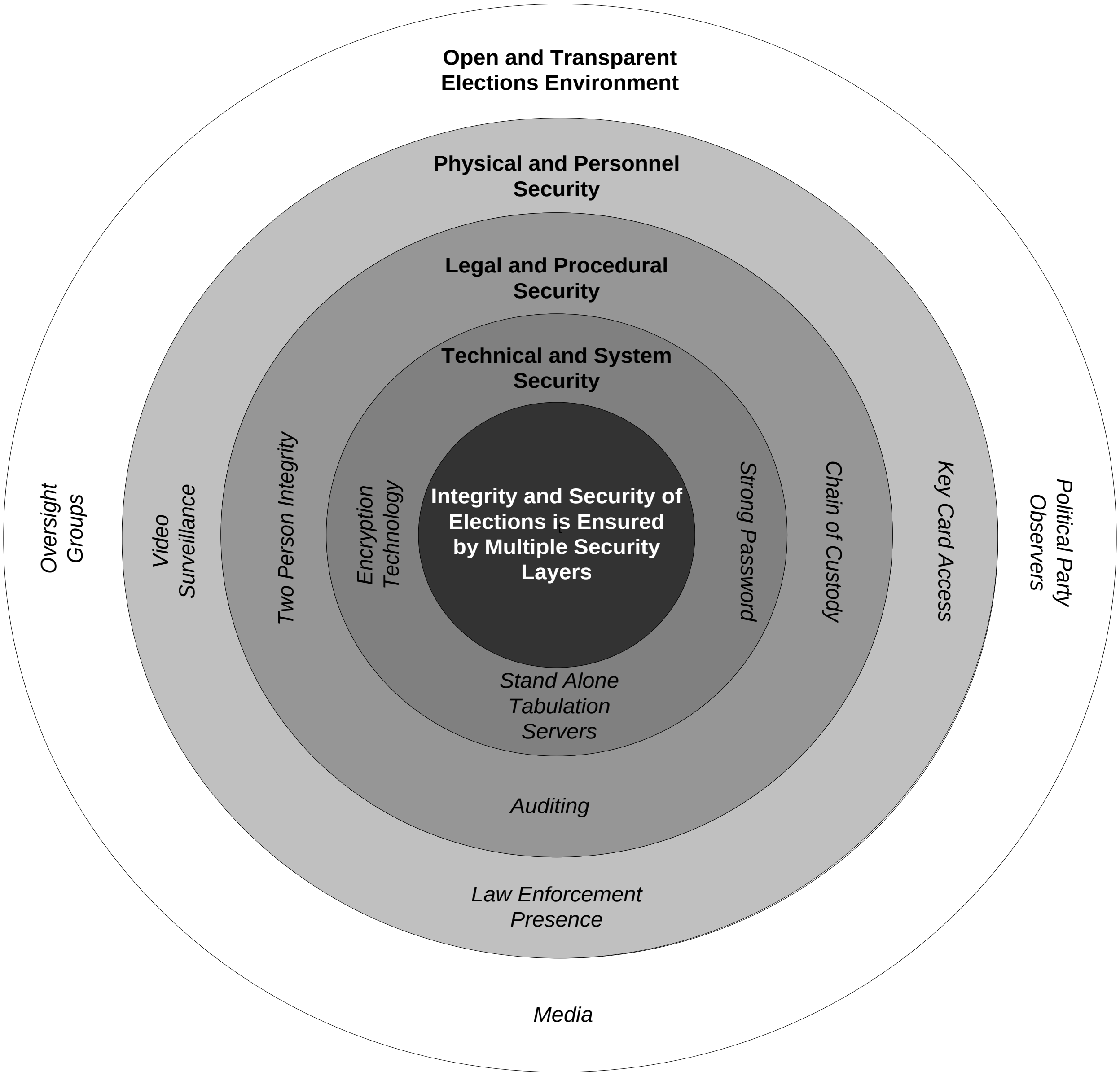
Open and Transparent Elections Environment
Physical and Personnel Security
Legal and Procedural Security
Technical and System Security
Integrity and Security of Elections is Ensured by Multiple Security Layers
Oversight Groups
Video Surveillance
Two Person Integrity
Encryption Technology
Strong Password
Chain of Custody
Key Card Access
Political Party Observers
Stand Alone Tabulation Servers
Auditing
Law Enforcement Presence
Media

Figure 1

Open and Transparent Election Environment

Administering elections is a monumental responsibility and one in which openness and transparency is essential to gaining and retaining public trust in government. It is the process by which citizens of a democratic republic choose their political leaders, and in the State of Washington, it is a system in which the electorate, through the process of initiative and referenda can directly make law. In any other system or process, it would likely be considered contradictory to require openness and transparency around a set of processes while at the same time restricting access and ensuring strong security, but this is exactly what election administrators across the nation must accomplish. For election administrators, openness and transparency are defined literally, they involve a variety of concepts that combine accountability, security, transparency, and accuracy, to enable access, foster openness, and preserve the integrity of the process. In King County, this is achieved through:

- Building infrastructure design and access
  - Open floor plans, viewing windows, transparent security cage material, and optimized viewing areas are all design elements that facilitate transparency. King County's new consolidated elections facility allows for accessibility, openness, and transparency. Most notably, the new facility features an observation loop around the perimeter of the entire second floor providing the public a view of all ballot processing activities. Additionally, available parking and transit serviced facilities helps minimize barriers that might prevent interested stakeholders from observing various aspects of election processing.
- Observers/Paid political party observers
  - The requirement for official Observers of the Election Process is grounded in state law. The responsibility for providing the official Observers is with the chair of the county major political party central committees, which he or she may delegate to a Chief Election Observer from the committee staff. Any other Observers are public Observers and are covered under separate policy. It is the responsibility of the Elections Director to designate the locations where the Observers are to be stationed, to approve the assignment of the Observers, and to provide training opportunities.
  - <u>Functions of Observers</u>: Observers serve as a check and balance against ballot fraud by watching to ensure that voted ballots are not altered from the way that they were voted by the voter, that no properly voted ballot is rejected from the Election Process without authorization of the County Canvassing Board as provided in RCW 29A.62, nor that any other ballot is added to or substituted for the legitimately voted ballots except as provided by law. Each Observer shall also serve to witness the action of the other. This applies to substitute Observers as well when used.
- Documentation of policies and procedures
- Public disclosure of records
- Media access and interest
- Oversight Groups

Physical and Personnel Security

The first line of defense against unauthorized access, tampering with elections results, or other illicit activity is physical and personnel security. Preventing unauthorized individuals from accessing areas or systems where election activity takes place protects the process from tampering. Ensuring that Elections personnel do not inappropriately influence or tamper with results starts with selecting highly trustworthy individuals and continues through additional layers of checks and balances that ensure individuals have neither the opportunity nor the inclination to harm the process.

Physical

Access Control: Access to the Renton Elections office and work areas is limited. The building has been divided in to different zones – public, secure, and highly secure. All exterior entrances, all doors from public to secure entrances and all entrances to highly secure areas are protected with key card readers. Additionally, doors to highly secure areas require a fingerprint to gain access. Each use of an access card is recorded in Ccure, King County's centralized building access security system, monitored 24/7 by the DES Facilities Management Division. These access records are maintained for three years.

All regular and long-term temporary employees are issued a biometric (with fingerprint) badge in addition to their regular King County ID. A select few short term temporary employees who require access to highly secure areas are also issued a biometric badge. This biometric badge allows them to open doors to only the areas that they are authorized to enter. In addition, all regular employees are required to display identification at all times.

Authorization to approve requests for biometric ID cards and to assign permissions to doors is limited to a very few individuals designated by the Director of Elections. This authorization is provided to King County Security in writing.

Visitors and temporary employees are checked in by Elections staff and issued temporary access cards with access limits based on the type of visit or job being performed.

Most doors are equipped with sensors that transmit an alarm to the security dispatch center if they are held open for more than a specified period of time (normally 30 seconds). An alarm will result in a phone call from Facilities Management to designated Elections' manager(s). Doors that require controlled access but cannot be locked (emergency exit doors, for example) are equipped with audible alarms in addition to transmitted alarms if opened without the use of an access card. Note that such unlocked doors only allow exit from secured areas, never entrance.

The Renton building is divided into security zones which can be armed and disarmed separately. These zones are protected by door sensors and motion detectors. The ability to arm or disarm is limited to specific individuals as specified by Election Program Managers. Once armed, any entry into the zone, even by employees usually authorized to enter, is considered a violation and will result in a phone call from Facilities Management to designated Elections' manager(s). Each violation is investigated before the zone is re-armed.

All temporary Elections staff, non-credentialed Elections personnel (including building maintenance personnel), and visitors/observers are required to enter the ballot processing areas through a central turnstile entrance that records this movement. At these turnstiles is a set of locked doors that closes off this entrance for complete security. Visitors and unofficial observers are required to be escorted through ballot processing areas.

To facilitate operational needs, doors can be unlocked and alarms bypassed. One-day requests for unlocking and bypassing alarms may be made to the Emergency Dispatch Center (EDC) by specified individuals (currently managers and supervisors). Long term requests must be made by a much more limited group designated by the Elections Director.

Access to the King County Data Center, housed in the Seattle Municipal Tower, is controlled by cardkeys and limited to Office of Information Resource Management (OIRM) staff. All non-OIRM personnel are required to sign in before being admitted and to be escorted by OIRM personnel.

Uniformed Security Presence: Commissioned law enforcement officers in uniform are assigned to the Renton Elections office and provide on-site security once voted ballots are returned for processing. As with Observers, their hours of operation are tied to the unsealing and sealing of ballot cages. During high volume processing, additional officers may be assigned to ensure full coverage.

On Election Day, uniformed guards (either off-duty police officers from the City of Seattle, Facilities Management Security Officers or King County Sheriff's Office deputies) are stationed at key points to protect the entry and exit points of elections buildings being used for critical functions. They are present during election ballot counting and transportation of ballots. The security function for various facilities is coordinated between the Elections Program Managers, a Facilities Management Division Elections Security Coordinator, and the King County Sheriff's Office Special Operations Section.

Video Surveillance: The Renton Elections office is equipped with 59 security cameras providing video surveillance of the exterior of the building, high secure areas, front counter, and warehouse.

All video is recorded 24/7 to a DVR that will be retained for same period of time required for other elections material. For federal election, this is 22 months and for all other elections 60 days.

Key Control: All keys to Election spaces are tightly controlled and distributed to individuals with a demonstrable need for access to the secured area(s). A record of who has been issued a key is maintained. Keys and county identification are collected upon termination. Should a keyed door be compromised through the loss of a key, Elections staff will take immediate action to have the appropriate door(s) re-keyed.

Accessible Voting Units (AVUs): Accessible voting units voting equipment are stored in a secured limited access warehouse facility. Voter access, supervisor, and administrator cards for the AVUs in addition to memory cards for each unit are secured in a locked room with limited access.

The outer case of each of these units is sealed with uniquely numbered, tamper-evident seals. Each of these units, in addition to the associated components, are tracked with an electronic inventory system to maintain a documented chain of custody.

Pursuant to state law, the accessible voting units create a voter verifiable paper audit trail during the voting process that is securely maintained for the legal retention period. This process is similar to the one used for optical scan paper ballots.

The voter verified paper audit trail is the number one recommendation by critics of electronic voting. This physical security of a voter verified paper audit trail combined with a transparent process, legal, procedural, and technical security measures combine to make a secure and accountable elections system that provides the blind or disabled the ability to cast a secret and independent ballot for the first time.

Personnel

Employees, volunteers and observers who work during elections must practice a high level of security. Only authorized personnel with a specific need for access are to be allowed in sensitive areas, including computer equipment rooms, ballot storage areas, and tabulation areas. Others will be accompanied by an escort in sensitive areas at all times.

To the extent allowed by law, police background checks are required for new hires, prior to employment, for personnel who work in areas of heightened security. Heightened security areas will be specified by the Elections Director in a separate document.

Training about areas of responsibility, sensitivity of information, security of ballots, and chain of custody for the ballots is necessary for all employees and volunteers, and is accomplished through individual work units in training and orientation by work group leads and supervisors.

All Elections personnel and observers are required to wear visible credentials at all times.

A dedicated elections staff recruiter focuses on hiring qualified temporary employees to assist with the various tasks of administering an election. Implementing core skills testing for temporary workers is a significant body of work, but it provides the recruiter with objective information that is used when placing temporary employees into various positions. Skills and abilities are matched to the positions resulting in greater performance, quality and efficiency. Although hiring temporary workers is dependent on the local job market, the more stringent hiring processes have contributed to an increased attention to detail and adherence to procedures. King County Elections will continue to engage in activities and processes that result in qualified workers being hired.

Legal and Procedural Security

Ballot Programming and Administration: All ballot programming and voting system administration is decentralized in Washington State. Elections staff programs and controls these processes in rooms under video surveillance with tightly controlled and tracked access. All election ballot programming and system administration is performed by qualified King County Elections staff. While vendor support personnel are at times on site for advice, they do not perform any actual functions related to the election. This is one of the key recommendations made in the Brennan Center report, “The Machinery of Democracy: Protecting Elections in an Electronic World.”

Ballot & Document Security: Voter affidavits are continually being processed in the elections office. When large deliveries of documents arrive they are opened and date stamped. They are then batched for scanning (signature & data capture). Once this process is complete, the batched documents are stored in trays and kept in locked storage cabinets for data entry. When work is being processed in the Elections office, it is removed from storage by supervisory staff and assigned to data entry personnel. At the end of each work shift, affidavits & documents are returned to the storage cabinets and locked.

Blank ballot stock, ballot stock, and live voted mail, as well as provisional ballots, are handled with many additional layers of security and accountability.

In the Elections office mail ballots are issued to voters over the counter using the Ballot-On-Request (BOR) module. Blank ballot stock used to print these in-house ballots is tracked by a stub numbering system and an audit log. This stock remains in secure storage when not in use. Only authorized elections staff have access to the blank ballot stock and the ability to issue ballots using the BOR module. This function is assigned only to full time elections staff. These individuals are specially trained to issue and produce ballots using the Ballot-On-Request (BOR) module. At close of business each day, the BOR operators log out of the system. The Superintendent of Elections or a designee is responsible for reviewing the audit logs and coordinating ballot accountability.

All live voted mail and provisional ballots and all printed ballot stock are secured in a cage when not actively being processed. Per the *Access Control* section above, these cages are secured with biometric key card access, which limits access and records ingress/egress on an access log. Only authorized personnel have access to these areas, and uniquely numbered seals are used to provide accountability of access.

Additionally, an electronic ballot may also be issued at any Accessible Voting Center. This ballot is issued, voted and cast on an accessible voting unit (AVU). AVUs are stored in similar cages when in the Elections office, or at an accessible voting center (AVC) during times of an election.

Accessible Voting Units: Only federal and state certified voting equipment is used in King County. Prior to deployment, all voting equipment is thoroughly “acceptance tested” using detailed checklists. Prior to acceptance and use, equipment is tested in a mock election and firmware is hash code tested to ensure that programming code delivered by the vendor is the same as that tested and certified by independent laboratories during the federal certification process. (See the Technical Security section for details about hash codes.)

In advance of every election all accessible voting units to be used in the election are tested to ensure that the logic and accuracy of the ballot programming is correct. This legally-required testing is conducted in the presence of political party observers and is open to the public. During this process memory cards containing the election-specific programming are sealed in the units' PCMCIA card slot with uniquely numbered tamper evident seals. The unique seal numbers are tracked from the time they are sealed in the warehouse by Elections staff until the units are returned by AVC staff on election night or the following day, depending on AVC breakdown timing requirements at each AVC. This enables King County to detect if the memory card has been disturbed or tampered with during the days in which the units are stored, at the King County Elections office or otherwise, prior to or during AVC operation.

The case of the AVU is also sealed with a second tamper evident seal to prevent undetected opening of the case. This ensures that no one has been able to access the internal components of the unit or been able to chance settings of internal controls (e.g. DIP switches).

Accessible Voting Center Security for Accessible Voting Units: Studies of jurisdictions that experienced problems with implementations of electronic voting equipment share a common theme of inadequate training and insufficient procedures. King County Elections carefully tracks lessons learned across the nation and has implemented best practices and security standards. In King County, each accessible voting center is staffed by sworn election workers, who have attended mandatory training. There are numerous checks and balances in place, including separation of duties as each voter moves through the AVC:

- The only form a ballot will take at an AVC is that of an accessible voting unit. This eliminates the need to secure and track hundreds of paper replacement or provisional ballots as was the case at each of King County's 392 polling places.
- Before opening each AVC, a "zero proof" printout from each voting machine verifies to AVC workers there are no votes stored on the memory card and that the races are properly coded for the election.
- A voter access card is issued only to qualified voters and not issued until proper identification is shown and it has been confirmed in the voter registration database that a mail-in ballot has not been returned or that the voter has not voted at another AVC. Only then is a voter access card programmed for the voting machine. A staff member guides the voter to an appropriate AVU and explains the machine to the voter. Staff monitors voters using the machine from an acceptable distance in order to be available to answer questions without compromising the privacy due to the voter. Staff is also tasked with detecting potential tampering with the machine.
- The voter access cards can only be programmed for one-time use and are collected after each voter is finished voting. Additionally, the voter access cards are programmed with a security key that is changed for each election.
- Additional Elections staff and equipment are on hand during days in which AVCs are operational to respond to AVU needs such as printer issues or to replenish supplies and troubleshoot problems.
- A summary report printout from each AVU confirms the total number of ballots cast on each unit. A canvassing of ballots cast and voters credited will be conducted daily.
- All rooms which house accessible voting centers are closed, locked and sealed with uniquely-numbered tamper-evident seals when the AVC is not in operation.
- Regarding the AVC at Bellevue City Hall, extra security measures are being installed. The City of Bellevue will install a deadbolt to which only King County will hold the keys.

When the AVC is not in operation, the deadbolt core will be removed to ensure that the integrity and security of the core is not breached.

- While Union Station has at least one security guard on the premises at all times, additional security personnel may be employed to further ensure security of the AVC during events held in the facility.

Ballot Drop Box Security: In preparing for the implementation of ballot drop boxes. King County Elections conducted firsthand research with multiple jurisdictions both in and out of Washington State. King County worked with its Disability Advisory Committee and other community members, and council staff in carefully deciding the locations for ballot drop boxes and accessible voting centers. Locations of ballot drop boxes were based on criteria such as security and accessibility. All ballot drop boxes are located at government facilities or well-traveled public areas and allow 24/7 access.

- Ballot retrieval staff, in teams of two persons, visits each box with sufficient frequency to ensure that deposited ballots are secure. The team visits each box at least once a day. During high volume elections, or as Election Day approaches, teams will visit each box multiple times per day.
- Internal ballot containers (the receptacle into which the ballot falls after being deposited) are sealed before being placed in each ballot drop box. By doing this, Elections personnel can confirm, via uniquely numbered, tamper-evident seal that the internal ballot container, has not been compromised. This seal number is recorded before the internal ballot containers are placed in each ballot drop box and tracked through the entire process until the internal ballot container is opened and the ballots removed at the Elections office.
- Ballot drop boxes are always examined, opened and the sealed internal container is removed for transport.
- All ballot drop boxes are located in well-lit areas.
- King County Elections is in regular contact with ballot drop box host facilities. Staff at each host facility are strongly encouraged to report any potential problems or ask question at any time—during an election or otherwise.
- Some ballot drop-off locations have security officers. Lake Forest Towne Centre and Crossroads Mall in Bellevue have roving security guards on the premises.

Post Election Audits: Prior to certification of each election a random audit of 4% of the accessible voting units deployed in the election is performed. The audit compares a hand recount of the voter verified paper audit trail against the electronic accumulation of results. This is another of the recommendations made in the Brennan Center report, “The Machinery of Democracy: Protecting Elections in an Electronic World.”

Ballot Tabulation System and Central Count Equipment Testing: Prior to every election, the GEMS database and central count tabulation equipment are subjected to extensive testing that culminates with the official Logic and Accuracy Test the Friday (four days) before the election. This rigorous testing procedurally checks that the database and each machine properly records, counts and tabulates results correctly. Each central count device must pass logic and accuracy testing. An extensive audit trail is maintained of this process including detailed checklists. The Logic and Accuracy test of the GEMS database and central count tabulation equipment is conducted in the presence of political party observers and is open to the public. During the primary and general elections, the Office of the Secretary of State is present for the Logic and Accuracy test.

Additionally, a Logic and Accuracy test is conducted mid-way through the election and immediately after certification of the election to guard against “time-bomb” coding that would allow a satisfactory test prior to the election but change processing after Election Day.

Two Person Rule: To ensure against the possibility of the illegal manipulation of voted ballots or AVUs, any time voted ballots are not in a sealed container in a secured area during the Election Process, they are in the presence of no fewer than two observers who are not of the same political party. Ballot processing shall not be curtailed if the requested Observers have not been provided. The Superintendent or Elections Program Managers may assign pairs of observers at times other than as prescribed above when in his or her opinion, it is warranted.

At any other time ballots in sealed containers are not secured in a vault, they are in the presence of at least two Elections Department staff members.

External Data Storage Mediums: Procedures have been created related to the manual handling, storage and disposition of data transfer medium (CD, DVD, disk) for security touch points related to DIMS. These procedures are located in the DIMSNeT Operations and Maintenance Plan, portions of which are available by request through the Superintendent of Election’s office or the Elections Director’s office.

Technical and System Security

The technical security features include the computer security components, plus the best practice tools, processes, procedures, and policies necessary to ensure data integrity and security of Elections technical systems and to prevent unauthorized access. Proper management of the technical security environment is critical to protect elections systems and data. Although the other layers of security would restrict access and facilitate detection (e.g. armed Sheriff's deputy security, camera surveillance, and key card access records), technical security is the last barrier to someone intent on malicious action.

General

Passwords: Per county IT policy, all systems and users are required to use passwords to log on to workstations, the network and all systems. Passwords must be "strong" passwords. A "strong" password is one that:

- is at least eight characters,
- uses at least three of the following: uppercase letters, lowercase letters, numbers, or special characters (e.g. #, @),
- is not a user's (or user's family) first or last name, birthday, phone number, part of an address, or user's login, and
- can not be found in a dictionary.

County policy requires that network and Windows passwords be changed at least every 90 days. This policy is enforced by Active Directory software. When changed, a password must be sufficiently different than the last six passwords used.

Elections policy requires that passwords are never to be written down unless they are kept in a locked container. Passwords are never shared. Any password that is suspected to have been compromised will be changed immediately, and audit logs checked to determine if anyone inappropriately accessed the system or data and if any malicious modifications were made. Supervisors must immediately notify Technical Services when any employee is released, particularly if they are released under adverse conditions, so that system access can be terminated.

All system and other critical passwords are to be securely recorded, in case of absence of critical personnel. They are written and sealed in such a way that tampering will be evident, and stored in a locked container in Technical Services. In the event that emergency access is required to a password protected system, permission must be obtained from the Technical Services Manager, Election Superintendent, or Director. For the GEMS tabulation password, the Program Manager of Ballot Processing and Delivery may also grant permission to open a password envelope. In the event that a password envelope is opened, the password will be changed at the earliest opportunity.

GEMS passwords are changed several times for each election cycle. A new password will be used when an election is initialized, immediately prior to the official Logic and Accuracy (L & A) test, and upon certification of the election. Between the official L & A Test and certification of the election, two-person integrity will be required for access to the GEMS database – that is, the GEMS server password and the GEMS database password will never be known by the same individuals. The server password will be set and known by Ballot Processing and Delivery personnel and the GEMS database password by Technical Services personnel. For the tabulation GEMS server, an additional password envelope is prepared, sealed and signed, and is in a ballot storage cage in a container that is only accessed in the presence of observers.

Anti-Virus Software: All King County systems and workstations have anti-virus software installed (with the exception of GEMS – discussed in the following paragraph). The software is set for automatic updates, so virus definitions are kept up to date.

The tabulation and development GEMS servers are not attached to any external network. In a closed system, virus infection is extremely unlikely but possible. However anti-virus software could potentially affect the GEMS system operation. Premier Elections Systems Inc. (PES) has recommended that King County install and run the anti-virus software during installation of any software or updates, and then remove the software from the GEMS server. By removing the software, it would remove any potential viruses but also prevent anti-virus software from affecting GEMS operations.

Security patches: It is mandatory that any workstations and systems attached to the county network receive Windows XP operating system patches validated and distributed by the Office of Information Resource Management (OIRM) LAN & Desktop Support group. For all workstations and servers other than GEMS this is accomplished automatically by OIRM over the network. Laptop users must exercise care that their computers are updated if computers are undocked when updates are pushed out. Since the GEMS servers are not attached to the network, they do not automatically receive patches. The GEMS servers have no external access, so Windows weaknesses cannot be exploited. Therefore it has been determined to be a greater risk to bring in external media that may contain viruses in addition to the patches, than to leave the servers unpatched.

Data backup: It is essential that data be backed up frequently so it can be restored in the event of catastrophic failure to computer or storage systems, or accidental deletion. A copy of the backup should also be stored at a second site in the event the primary site suffers damage rendering the backup unusable. For systems connected to the county network, OIRM provides this service for network disk drives and for servers (e.g. DIMS) they operate on our behalf. The DIMS System Administrator will request additional complete back ups that coincide with significant events in the election cycle.

GEMS servers are not attached to the network. As a result, OIRM does not back up these databases. It is the responsibility of the GEMS systems analyst(s) to perform frequent backups, particularly at critical election events. GEMS backups during tabulation are discussed in the GEMS section. Specific backups during the development and testing periods are covered in separate Elections procedures.

Certification: All software and hardware involved with collecting and tabulating votes must be certified both by the federal government (currently by the Election Assistance Commission) and Washington State Secretary of State. Currently King County uses the following items that must be certified: GEMS software, AccuVote Optical Scanner and firmware, AccuVote –TSx touch screen hardware and firmware, and Express Poll 2000. Any upgrades to this equipment must also be certified. In addition to state and federal certification, King County Elections performs acceptance tests on any new or upgraded hardware or software before placing it in service.

Hash Codes[1]: Hash code testing validates that the ballot tabulation software is exactly the same as the software tested and analyzed in the federal and state certification process, and provides election administrators and observers in King County with the assurances needed to be certain that no changes to applications or other critical files have occurred.

[1] A hash code is the result of running data or the object code for an application through a mathematical algorithm. This hash code is unique to that set of data or object code. Changing only one bit of information will result in an entirely different hash code. It is similar to an electronic signature.

Before installing or upgrading any software on any system involved with collecting and tabulating votes, King County Elections uses hash code testing to verify that the software received is the same as that certified.[2] In addition to testing software on receipt, King County Elections performs periodic hash code testing of a percentage of randomly selected devices for each election to verify that software installed is the certified version and has not been tampered with. A listing of valid hash codes for certified software can be found at the National Institute of Standards and Technology (NIST) web site - http://www.nsrl.nist.gov/vote.html.

See the GEMS section below for hash code usage during election tabulation.

Workstation Security: Except for ballot tabulation work, the majority of the work done in elections occurs on desktop workstations connected to networked business applications (e.g.DIMS), so workstation level security is an important part of the overall security picture. Users must adhere to the following practices at the workstation level:

- Follow the password policies discussed earlier
- Always lock their computer (or common use computers such as the front desk) when leaving their workstation
- Never install software on their workstations that has not been approved by Technical Services
- Maintain up to date anti-virus definitions and software. Never turn off anti-virus protection
- Do not install any additional hardware unless approved by the Technical Services Manager. In particular, never install any modems or wireless devices.
- All employees are to have read and acknowledged the King County computer acceptable use policy

Laptops: Laptops because of their portability present unique challenges in the security arena. A laptop will frequently be out of areas that are physically secure, and in the event of loss or theft leaves information more susceptible to compromise. This unique vulnerability requires additional restrictions. The storage of personal identifying information on a laptop is prohibited unless the information is stored in encrypted format.

No non-county employee laptops are to be connected to the county network unless review by LAN Administration staff prior to connection. The county does not provide public Wi-Fi at the Renton Elections Office.

The laptops used at the Accessible Voting Centers (AVC) are configured with McAfee Host Intrusion Prevention Software (HIPS) and will have McAfee hard disk encryption when available from the Office of Information Resource Management (OIRM). The Voter Registration Application (DIMS) requires an authenticated domain login for its connection the DIMS application server. AVC staff will use the laptop during training while connected to the King County network so their King County domain credentials are cached on the laptop and will be available while at the AVC. Local Windows XP operating system accounts will not be used on the laptop while at the AVC.

Network

Interconnectivity of King County Election's workstations with various election systems servers and connectivity between Elections and the rest of King County is accomplished using the

[2] All software currently in use has been hash code tested and verified.

county data network. Because of the network infrastructure design and safeguards, the use of Active Directory, and other technical best practices, significant barriers exist to help prevent unauthorized access to elections systems and data.

Security of the network is the responsibility of the Office of Information Resource Management (OIRM), Network, Systems and Operations group (NSO). Changes to improve security or rectify problems with existing security arrangements should they arise would be the subject of negotiations between Elections Technical Services and OIRM-NSO.

Architecture*[3]*: The transmission of data between the OIRM data center, the Renton Elections Facility, and the Accessible Voting Centers (AVCs) is carried over I-Net or the KC WAN. The I-Net uses fiber channel leased from a commercial carrier. All switches, routers and other network equipment are King County owned. The KC WAN utilizes King County owned lines. Both the I-Net and the KC WAN are administered by King County OIRM. Routers and switches are in locked wiring and data communication equipment closets to ensure unauthorized individuals cannot get to open ports or areas where they can tamper with the network equipment or configuration.

Connection to the Internet is accomplished through the use of a firewall at the county Data Center. This firewall protects workstations, servers, and systems on the internal network against attacks from the Internet. Measures implemented within the firewall shield IP addresses from the internet reducing the potential for successful malicious activity from external sites. The county also performs anti-virus scanning and intrusion detection at the firewall.

Servers and software used for the tabulation of ballots and the reporting of results (i.e. GEMS) are not connected to the Internet, the county's intranet, or the internal building LAN. The local area network for tabulation purposes consists only of tabulation hardware and a local printer. All are physically located in the same space, secured in a separate locked and access-controlled tabulation room.

Election connectivity is via subnet(s) unique to Elections. This provides a measure of protection from problems/attacks affecting other agencies.

Restrictions: The use of modems on the King County network are prohibited both by OIRM and Elections. In the event there is no other way to establish a network connection, the use of a modem anywhere within Elections must be approved by the Technical Services Manager and the county's Chief Information Officer (CIO). Any use of a modem will only be permitted if there is absolutely no other way to establish communications and will require stringent conditions to ensure adequate security. There currently are no such exceptions authorized.

Users with legitimate needs to connect to the network from external locations will be provided with Secure Socket Link Virtual Private Network (SSL-VPN) accounts. VPNs use tunneling technology with encrypted links to protect the data transmissions. They also use the Active Directory authentication to ensure only authorized users are permitted to connect to the network.

The Accessible Voting Centers located at the City of Bellevue and Sound Transit/Union Station will use the host agency local network/Internet connection to establish a SSL VPN connection to the King County Network. For these laptops, the SSL VPN connection

[3] Detailed architecture diagrams and specifications are included in a separate document that has restricted distribution.

administered by OIRM will be configured for the limited traffic to the Voter Registration Application (DIMS) SQL and file server.

There are no wireless devices used within the tabulation system or with any voting device. To prevent any perception of such (through detection of signals with sniffers), wireless technology is prohibited from being used within the Renton Elections Office. The use of wireless access points on the Elections subnet portion of the network is prohibited.

DIMS

DIMS is a fully integrated election management system used to manage voter, jurisdiction, precinct, and contest functions. In addition, DIMS is a key source of initial (candidate and jurisdiction) information for election preparation in GEMS. DIMS data, most of which is considered public information, and the DIMS application, are protected by barriers such as network architecture design, user authentication and use of Active Directory to manage permissions, external access restrictions and protocols, and detailed event logs.

DIMS does not have any functionality related to vote tabulation or any data related to votes cast. For that reason it does not come under the same scrutiny as GEMS does and is not subject to some of the more stringent requirements (such as federal certification).

User Authentication: DIMS maintains its own authentication system that governs not only who can log on, but also what rights they have once they have been authenticated. DIMS relies on the Windows password. Within DIMS, internal permission tables govern what subsystems and menus the user has access to and whether they have read only or modification rights. The DIMS administrator, a Technical Services employee, maintains these permission tables based on the workgroup supervisor's determination of the appropriate access level required to perform their job. DIMS logs all user actions including the end user's login-id, date/time stamp, and data values before and after the change.

Installed Software: Internet Information Services (IIS) software is prohibited from being installed on any DIMS server. This closes a potential vulnerability for unauthorized users to access the system.

External Access: Access to Elections' separate subnet will be granted to the DIMS service engineer for database administration and maintenance using the county's VPN network. The DIMS service engineer is required to notify Technical Services whenever they will modify the database and obtain positive consent before making the change.

Access may also be granted to the DIMS vendor (Premier Election Systems) for debugging or installation of vendor-supported software. Access is granted for a specific time window and purpose, and must be accompanied by a signed, dated "VR System Access Authorization Form" faxed or emailed to Premier, with a copy to OIRM DCS.

Business Continuity: The DIMS test server is capable of serving as the DIMS production server in the event of failure. Data is backed up daily (weekly full, daily incremental) providing for restoration of data with a maximum of 24-hour loss.

External Data Sources: The Washington State Office of the Secretary of State (OSOS) operates the state's Voter Registration Database (VRDB) which is tightly integrated with DIMS. VRDB pushes transactions to DIMS from the Motor Voter program and the State's online voter registration system, and receives a transaction for every update made in DIMS. Incoming transactions are not processed automatically; they are reviewed and processed individually by Voter Services personnel. There is no ability to directly update DIMS via the VRDB link. Lapses or breaches in OSOS's VRDB security could potentially cause good data in DIMS to be overwritten by corrupt data from VRDB, but only to the extent that the data was formatted correctly and contained believable content.

Other external data sources (LexisNexis, the Washington State Department of Licensing, the U.S. Social Security Administration) are accessed as research tools, but do not have any system connection to DIMS. Because of the sensitive nature of the data involved, their use is limited to key Voter Services personnel.

GEMS

GEMS (Global Election Management System) is a comprehensive system used to design and build ballots, tabulate absentee ballots, accumulate results from Accessible Voting Centers, and report election results. GEMS is also used to print ballots for over the counter absentee and provisional ballots.

GEMS is the most secured system in use by King County Elections because of its role in tabulating and reporting election results. The hardened physical security measures significantly restrict unauthorized access, and since the tabulation equipment is not networked to any other system, physical access to the server would be required in order to attempt any unauthorized access. Access logs, log-on credentials, logic and accuracy tests, and hash code testing are all additional measures taken by King County to create a barrier, minimize or eliminate opportunity, and provide for the security and integrity of the tabulation system.

Architecture*[4]*: GEMS is installed on only a limited number of workstations/servers. GEMS is installed on two primary servers within the Renton Elections office – one in a secured room in the Technical Services area that is used for development of ballots and testing, and the other in the secured tabulation room in the Ballot Processing area that is used for final testing and tabulation. There is a backup server at each location. Neither of these servers nor their backups are connected to an external network (i.e. outside their secured rooms) and are prohibited from being so. Any sharing of data files (to the website, Secretary of State, or for other administrative reporting) is done by using portable media, such as CD or diskette. Internal networks exist with each set of servers in the way of printers, AccuVote scanners, and AccuVote TSx Accessible Voting Units (AVU). The use of wireless networking devices on any GEMS server is strictly prohibited.

In addition to these servers, GEMS is also installed on five workstations for specific business purposes:

- Two workstations at the front counter in the Voter Services area for Ballots on Request
- A workstation in the Ballot Processing area for Ballots on Request
- Two workstations in the Ballot Processing area for administrative reporting

GEMS will not be installed on any other computers without the express consent of the Technical Services Manager.

Configuration and Implementation: Several restrictions are imposed on the equipment and operation of GEMS servers and workstations. These are necessary to ensure a higher than normal level of security for systems involved in tabulating results or that can produce ballots whose distribution must be controlled once printed.

[4] Detailed architecture diagrams and specifications are included in a separate document that has restricted distribution.

BIOS: A BIOS password is assigned on all GEMS servers. Further, the BIOS is configured to ensure the boot (startup) sequence is restricted to the internal hard drive, thus preventing booting from unauthorized removal media (e.g. CD, floppy diskette, USB device).

Installed software: Only software required to operate GEMS or to enhance the security of the system is installed on the GEMS tabulation and ballot development servers. Specifically, Microsoft Office, Microsoft Access, and any other software that enables users to work with Direct Access Objects (DAO) or ActiveX Data Objects (ADO) are strictly prohibited. Although GEMS uses the Jet 4.0 database engine (e.g., Microsoft Access database engine), MS Access is NOT installed on the GEMS servers used for tabulation or ballot development. Installation of IIS on GEMS servers or workstations hosting GEMS is prohibited.

Use of Access Software: Use of Microsoft Access with GEMS will be limited to the two workstations that are used to produce administrative reports[5]. Access is never used directly on the GEMS database - the data is retrieved through the use of a read-only connection to GEMS from a separate Access application.

System Configuration: Prior to the official Logic and Accuracy test, the configuration of the tabulation system is documented in accordance with other Elections procedures. After the L & A Test, the configuration of the tabulation system will not be modified without the express consent of both the Technical Services Manager. Any approved modifications will be documented on the System Configuration Log, and notification of modifications will be sent to the Office of the Secretary of State and the King County Canvassing Board. If significant changes are made, a new Logic and Accuracy test will be conducted according to the established process.

Tabulation Operations: During election tabulation, additional steps are taken to ensure the security and integrity of tabulated results whenever there is an interruption in operations. The output at the start of the interruption is compared to the output when activities resume, in order to validate there has been no change in the interim. Elections personnel and political party observers view and validate the output, and party observers initial or sign reports as appropriate to attest to their validation.

- GEMS Cards Cast Report is produced at every interruption (lunch, database backup, end of day, etc.)
- GEMS database backup to CD (using new, shrink-wrapped CD's) is produced at the end of day, and the database is restored from CD at the beginning of the next day
- Hash Code of GEMS software is produced at the beginning and end of the day
- Hash code of the GEMS database backup file is produced at the end of the day

These steps are documented in more detail in separate Elections procedures.

Similar steps are taken in the event of a power failure and are documented in a separate Elections procedure.

Audit Logs: Before the Logic and Accuracy Tests, the Window's audit logs for the tabulation server will be cleared. During the tabulation process, these logs will not be

[5] The ability to use GEMS data outside of the GEMS tabulation environment is necessary because GEMS does not have sufficient reports to meet the various needs of elections administrators, council, and other groups. Since GEMS itself is required to be certified, making quick changes to meet the imposed reporting requirements (either by Diebold or internal staff) is unrealistic.

cleared. After certification, the logs will be printed and kept with other election records for the retention period required for other materials for that type of election.

Business Continuity: As discussed in the architecture section, each primary server is paired with a backup server. In addition, each primary server can serve as a backup to the other. However, since neither server is attached to the network, the database would need to be transported to the other site by removable media (e,g. CD). Application software on the two primary servers is to be maintained in an identical state.

The tabulation room GEMS server is served by an uninterruptible power supply (UPS) to facilitate an orderly shutdown and securing of the GEMS database, which would include creation of a Cards Cast Report, hash coding, and backup to CD.

Pitney-Bowes Sorting Equipment

The Pitney Bowes Sorting Equipment for returned mail ballot packets includes two large 32-bin Olympus II sorter/scanners and the computer equipment necessary to run the software applications that manages the sorters, captures scanned images and provides tracking data for every returned ballot packet that is processed through the sorters. The system is called Relia-Vote

The Relia-Vote system hardware consists of both standard workstations and a server that are connected together on a local network. The Relia-Vote system hardware and software on the local network is not part of the King County domain and is administered by an on-site Pitney Bowes Technician.

The Relia-Vote Server (in-addition to its own local network connection) has a 2nd network connection to the KC Wan. Access to the Pitney Bowes operating/file system by Elections staff is controlled by local accounts on the Relia-Vote Server administered by Technical Services following OIRM password management guidelines. Authorized Ballot Processing staff copy files between the Relia-Vote Server and servers on the KC network to facilitate the flow of data between the Relia-Vote system and the Voter Registration Application (DIMS).

Accessible Voting Units (AVUs)

By administrative code, voting units deployed in Washington State are not equipped with wireless technology. Pursuant to state certification requirements, in order to tabulate votes the memory cards from the accessible voting units are uploaded directly to the GEMS server. King County no longer uses modems to transfer results from remote sites to the central GEMS server.

The tabulation systems for AVUs utilize a Key Card Tool encryption program that sets an encrypted code that is required for any voter access, supervisor, administrator or memory card to be used in a device. This code is changed prior to each election by Elections staff.

Summary

Effective security does not rely on a single process, feature, or policy. Effective security requires a number of interrelated processes, systems, and policies that complement and build on each other. The systems, process and policies that comprise layers of security for King County Elections are represented in detail throughout this plan, and illustrated graphically in the Layers of Election Security diagram, Figure 1.

These multiple layers of security systems, processes and/or procedures ensure that elections are not inappropriately influenced. External stakeholders such as the media, party observers, elections oversight groups, the Office of the Secretary of State, and the public provide transparency and are integral to the detection of problems with the elections process. The physical and personnel security measures which have been implemented ensure that only authorized individuals are allowed access to critical election spaces, materials, technical systems, and ballots. Elections staff, both permanent and temporary, are trained in elections processes and procedures designed to ensure the security and integrity of the election process. These elections processes are audited and reviewed throughout, with many checkpoints for accuracy. This layered approach ensures that if one or even two layers are compromised, bypassed, or proven ineffective, the security and integrity of the election process is still preserved.

This Security Plan details the many safeguards in place that protect elections in King County. Many of these safeguards are not unique to King County Elections; they are deployed throughout election agencies across the state and country. Although many of the safeguards in place today were implemented before they became recognized best practices or recommendations by outside stakeholders, they are nonetheless based on lessons learned internally, through observation of others, or were existing legal requirements.

The security of elections in King County is also the result of a genuine commitment by election administrators to cooperate with outside stakeholders. Local stakeholder recommendations for improvement have proved beneficial and many have been implemented. King County Elections continues to be receptive to recommendations made by all interested parties in so much as they positively contribute to election security, election integrity, public trust, openness, transparency, and accountability.

Election administrators and public officials continue to implement and improve safeguards to protect the integrity of elections, as all share responsibility for protecting this process.   A key element to improving election security is the participation of voters, state and local officials, political parties and other stakeholders all working in tandem with election officials to identify security threats and areas of opportunity for improvement.

Appendix A – Guiding Laws, Policies and Best Practices

Laws, policies and best practices that apply to elections include:

- Help America Vote Act of 2002 (HAVA): 42 U.S.C. 15301 to 15545 http://www.eac.gov/law_ext.asp
- RCW Title 29A – Elections http://apps.leg.wa.gov/rcw/default.aspx?Cite=29A
- WAC Chapter 434 – Secretary of State http://apps.leg.wa.gov/wac/default.aspx?cite=434
- KCC Title 1, County Council and Elections
- KCC 2.16.035, Department of Executive Services
- Department Policies and Procedures for the Records, Elections and Licensing Services Division, PER 9-2 (DP)
- King County Elections policies & procedures
- Quick Start Management Guide for Voting System security, U.S. Election Assistance Commission - http://www.eac.gov/docs/EAC%20Security.pdf
- Brennan Center report, “The Machinery of Democracy: Protecting Elections in an Electronic World,” – http://www.brennancenter.org/dynamic/subpages/download_file_36343.pdf

Appendix B – Responsible Agencies and Roles

Elections require participation and responsibility at all levels of government. The list of responsibilities below is not intended to be exhaustive but does provide an overview for various aspects of the elections process.

United States Government

- Elections Assistance Commission provides certification of voting tabulation systems

Washington State Government

- Office of the Secretary of State (OSOS) election review and advisory
- OSOS provides certification of voting tabulation systems
- Updates RCW Title 29A – Elections
- Updates Title 434 WAC – Secretary of State

Cities

- Local security used for jurisdictions with Accessible Voting Centers

King County Government

- Oversees federal, state, and local elections for geographic King County

King County Departments

Elections Office

- Primary responsibility for overseeing, monitoring and reporting results for elections held in King County
- The verification of absentee ballot signatures
- GIS staff will maintain the geographic boundaries of all major and minor jurisdictions in King County.
- Voter Registration Staff process voter registration affidavits and documents.

Department of Executive Services (DES)/Facilities Management Division

- Facilities Security Personnel shall assist the King County Sheriff for security at the King County Administration Building during elections as outlined in Facilities Security Policy and Procedure Manual, Section 5 Special Programs & Assignments, sections 5.95.0 through 5.95.6, July 2003.
- Provide security enhancements for King County owned facilities used for tabulation and verification activities.

Office of Information and Resource Management (OIRM)

- Administer and maintain the King County data network
- Provide network security administration
- Provide DIMS database administration and support

King County Sheriff's Office (KCSO)

- Provide security staffing at King County unincorporated locations and King County owned facilities

King County Prosecuting Attorney's Office

- Provide legal counsel